

WHAT IS CLAIMED IS:

Sub at
Sub D1

1 1. A method for inserting a digital signature into
2 digital data, the digital data comprising bits, the method
3 comprising the steps of:

4 assigning predetermined bits of the digital data
5 for receiving the digital signature;

6 signing the digital data excluding the
7 predetermined bits resulting in the digital signature; and

8 inserting the digital signature into the
9 predetermined bits of the digital data for subsequent
10 authentication of the digital data.

1 2. The method of claim 1, wherein the signing step
2 comprises:

3 applying a one-way hashing function to the digital
4 data excluding said predetermined bits resulting in a hash; and
5 encrypting the hash.

1 3. The method of claim 1, wherein the digital data is
2 selected from a group consisting of image data, video data, and
3 audio data.

1 4. The method of claim 1, further comprising the step
2 of inserting associated data into the digital data prior to the
3 signing step such that the digital signature authenticates both
4 the associated data as well as the digital data.

1 5. The method of claim 4, wherein the associated data
2 is inserted into the bits of the digital data excluding the
3 predetermined bits.

1 6. The method of claim 4, wherein the digital data
2 comprises a plurality of samples, each of the samples being
3 defined by a plurality of the bits, from a most significant bit
4 to a least significant bit, all of the least significant bits
5 defining the plurality of samples comprising a least significant
6 bit plane, wherein the predetermined bits comprise at least a
7 portion of the least significant bit plane.

1 7. The method of claim 6, wherein the digital data is
2 an image and each sample is an image pixel.

1 8. The method of claim 6, wherein the digital data is
2 video and each sample is a spatial temporal sample.

1 9. The method of claim 6, wherein the digital data is
2 audio and each sample is a time sample.

1 10. The method of claim 6, wherein the associated data
2 is inserted into at least a portion of the remaining least
3 significant bits in the least significant bit plane.

1 11. The method of claim 4, wherein the digital data
2 comprises a plurality of samples, each of the samples being
3 defined by a plurality of the bits, further comprising the step
4 of transforming the plurality of bits into an alternative
5 representation having at least first and second characteristic
6 components, wherein the predetermined bits comprise the first
7 characteristic component.

1 12. The method of claim 11, wherein the digital data
2 is an image and each sample is an image pixel.

1 13. The method of claim 11, wherein the digital data
2 is video and each sample is a spatial temporal sample.

1 14. The method of claim 11, wherein the digital data
2 is audio and each sample is a time sample.

1 15. The method of claim 11, wherein the associated
2 data is inserted into at least a portion of the second
3 characteristic component.

1 16. The method of claim 15, wherein the alternative
2 representation is a frequency domain representation having high
3 and low frequency components, wherein the first characteristic
4 component is a portion of the high frequency component and the
5 second characteristic component is the remaining high frequency
6 component and the low frequency component.

1 17. The method of claim 4, wherein at least a portion
2 of the associated data comprises data identifying a public key
3 needed to decrypt the digital signature.

1 18. The method of claim 4, wherein the associated data
2 comprises data identifying a source of the digital data.

1 19. The method of claim 4, wherein the associated data
2 comprises data identifying the identity of an owner of the
3 digital data.

1 20. The method of claim 19, wherein the digital data
2 is an image and the associated data comprises data identifying a
3 photographer of the image.

a 1 21. The method of claim 1, wherein a portion of the
2 associated data is encrypted and a remaining portion of the
3 associated data is unencrypted.

a 1 22. The method of claim 1, wherein the associated data
2 comprises at least two fields.

1 23. The method of claim 22, wherein at least one of
2 the fields comprises data identifying a public key needed to
3 decrypt the digital signature.

1 24. The method of claim 23, wherein at least one other
2 field comprises data identifying the owner of the public key.

1 25. The method of claim 1, further comprising the step
2 of receiving the associated data from an external source.

1 26. The method of claim 25, wherein the external
2 source is a Global Positioning Satellite transmission.

1 27. The method of claim 1, wherein the digital data is
2 compressed using a compression standard resulting in a
3 compressed file, wherein the method further comprises the steps
4 of:

5 creating a decompressed file prior to the signing
6 step; signing the decompressed file resulting in the digital
7 signature; and

1 28. The method of claim 27, wherein the digital data
2 is an image and the compression standard is JPEG.

1 29. The method of claim 27, wherein the digital data
2 is video and the compression standard is MPEG.

3 30. The method of claim 4, wherein the digital data is
4 compressed using a compression standard resulting in a
5 compressed file, wherein the method further comprises the steps
6 of:

7 creating a decompressed file prior to the signing
8 step;

11 signing the decompressed file resulting in the
12 digital signature; and

1 31. The method of claim 30, wherein the digital data
2 is an image and the compression standard is JPEG.

1 32. The method of claim 30, wherein the digital data
2 is video and the compression standard is MPEG.

1 33. The method of claim 4, wherein the digital data
2 comprises a plurality of samples, each of the samples being
3 defined by a plurality of the bits, from a most significant bit
4 to a least significant bit, all of the least significant bits
5 defining the plurality of samples comprising a least significant
6 bit plane, wherein the method further comprises the steps of:

7 ignoring the least significant bit plane in the
8 digital data;

9 concatenating the associated data to the digital
10 data having the ignored least significant bit plane prior to the
11 signing step;

12 performing the signing step to the digital data
13 having concatenated associated data resulting in the digital
14 signature;

15 wherein the predetermined bits comprise at least a
16 portion of the least significant bit plane and the associated
17 data is inserted into at least a portion of the remaining least
18 significant bits in the least significant bit plane.

1 34. The method of claim 1, further comprising the
2 steps of:

3 providing time data identifying the time the
4 digital data was created;

5 concatenating the hash and the time data;

6 applying a one-way hashing function to the
7 concatenated hash and time data resulting in a second hash; and

8 encrypting the second hash instead of the first
9 hash to result in a time stamp containing the digital signature,
10 wherein both the digital data and the time data are subsequently
11 authenticated.

1 35. The method of claim 34, further comprising the
2 steps of:

3 transmitting the hash and signature to a third
4 party for performance of the providing, concatenating, and
5 encrypting steps; and

6 receiving the time stamp from the third party
7 prior to the inserting step.

1 36. The method of claim 35, wherein the trusted third
2 party resides at an internet address and the transmitting and
3 receiving steps are done through the internet.

1 37. The method of claim 34, wherein the time stamp is
2 provided by a semiconductor chip having a tamper resistant clock
3 and a tamper resistant time stamping circuit, wherein the clock
4 outputs the time data which together with the digital signature
5 is signed by the circuit to output the time stamp.

1 38. The method of claim 4, further comprising the
2 steps of:

3 storing an identifier in a memory corresponding to
4 each of at least one user of a device which creates the digital
5 data;

6 recognizing a user of the device whose identifier is stored in
7 the memory; and

8 outputting the identifier corresponding to the
9 recognized user from the memory to be inserted as the associated
10 data.

1 39. The method of claim 38, further comprising the
2 steps of storing a private key for signing the digital data in
3 the memory corresponding to each user and using the private key
4 for signing the digital data.

1 40. The method of claim 38, wherein the recognizing
2 step is accomplished by a fingerprint recognition system.

1 41. The method of claim 38, wherein the identifier is
2 a name of the recognized user.

1 42. A method for authenticating digital data having an
2 embedded digital signature in predetermined bits of the digital
3 data, the method comprising the steps of:

4 extracting the digital signature from the
5 predetermined bits;

6 decrypting the digital signature from the digital
7 data resulting in a first hash;

8 applying a one-way hashing function used by an
9 encoder of the digital data to the digital data excluding the
10 predetermined bits resulting in a second hash; and

11 comparing the first hash to the second hash
12 wherein if the first hash matches the second hash the digital
13 data is authentic.

1 43. The method of claim 42, wherein the digital data
2 is selected from a group consisting of image data, video data,
3 and audio data.

1 44. The method of claim 42, wherein the digital data
2 further comprises associated data inserted into known bits of the
3 digital data, wherein the method authenticates both the
4 associated data as well as the digital data.

1 45. The method of claim 44, wherein the associated
2 data is inserted into the bits of the digital data excluding the
3 predetermined bits.

1 46. The method of claim 44, wherein the digital data
2 is compressed using a compression standard resulting in a
3 compressed file and wherein the digital signature and associated
4 data are contained in a header in the compressed file, wherein
5 the method further comprises the steps of:

6 decompressing the compressed file; and

7 replacing the signature and associated data from
8 the header into the predetermined bits and the known bits,
9 respectively, prior to the extracting step.

1 47. An encoder for inserting a digital signature into
2 digital data, the digital data comprising bits, the encoder
3 comprising:

4 means for assigning predetermined bits of the
5 digital data for receiving the digital signature;

6 means for signing the digital data excluding the
7 predetermined bits resulting in the digital signature; and

8 means for inserting the digital signature into the
9 predetermined bits of the digital data for subsequent
10 authentication of the digital data.

1 48. The encoder of claim 47, wherein the means for
2 signing comprises:

3 means for applying a one-way hashing function to
4 the digital data excluding said predetermined bits resulting in a
5 hash; and

6 encrypting the hash.

1 49. The encoder of claim 47, wherein the digital data
2 is selected from a group consisting of image data, video data,
3 and audio data.

1 50. The encoder of claim 47, further comprising means
2 for inserting associated data into the digital data prior to
3 signing the digital data such that the encoder authenticates both
4 the associated data as well as the digital data.

1 51. The encoder of claim 50, wherein the associated
2 data is inserted into the bits of the digital data excluding the
3 predetermined bits.

1 52. The encoder of claim 50, wherein the digital data
2 comprises a plurality of samples, each of the samples being

3 defined by a plurality of the bits, from a most significant bit
4 to a least significant bit, all of the least significant bits
5 defining the plurality of samples comprising a least significant
6 bit plane, wherein the predetermined bits comprise at least a
7 portion of the least significant bit plane.

1 53. The encoder of claim 52, wherein the digital data
2 is an image and each sample is an image pixel.

1 54. The encoder of claim 52, wherein the digital data
2 is video and each sample is a spatial temporal sample.

1 55. The encoder of claim 52, wherein the digital data
2 is audio and each sample is a time sample.

1 56. The encoder of claim 52, wherein the associated
2 data is inserted into at least a portion of the remaining least
3 significant bits in the least significant bit plane.

a 1 57. The encoder of claim 56, wherein the digital data
2 is an image comprising a plurality of samples, each of the
3 samples being defined by a plurality of the bits, further
4 comprising means for transforming the plurality of bits into an
5 alternative representation having at least first and second
6 characteristic components, wherein the predetermined bits
7 comprise the first characteristic component.

1 58. The encoder of claim 57, wherein the digital data
2 is an image and each sample is an image pixel.

1 59. The encoder of claim 57, wherein the digital data
2 is video and each sample is a spatial temporal sample.

1 60. The encoder of claim 57, wherein the digital data
2 is audio and each sample is a time sample.

1 61. The encoder of claim 57, wherein the associated
2 data is inserted into at least a portion of second characteristic
3 component.

1 62. The encoder of claim 61, wherein the alternative
2 representation is a frequency domain representation having high
3 and low frequency components, wherein the first characteristic
4 component is a portion of the high frequency component and the
5 second characteristic component is the remaining high frequency
6 component and the low frequency component.

1 63. The encoder of claim 50, wherein at least a
2 portion of the associated data comprises data identifying a
3 public key needed to decrypt the digital signature.

1 64. The encoder of claim 50, wherein the associated
2 data comprises data identifying a source of the digital data.

1 65. The encoder of claim 50, wherein the associated
2 data comprises data identifying the identity of an owner of the
3 digital data.

1 66. The encoder of claim 65, wherein the digital data
2 is an image and the associated data comprises data identifying a
3 photographer of the image.

1 67. The encoder of claim 50, wherein a portion of the
2 associated data is encrypted and a remaining portion of the
3 associated data is unencrypted.

1 68. The encoder of claim 50, wherein the associated
2 data comprises at least two fields.

1 69. The encoder of claim 68, wherein at least one of
2 the fields comprises data identifying a public key needed to
3 decrypt the digital signature.

1 ~~70.~~ The encoder of ~~claim~~ 69, wherein at least one
2 other field comprises data identifying the owner of the public
3 key.

1 71. The encoder of claim 65, further comprising means
2 for receiving the associated data from an external source.

1 72. The encoder of claim 71, wherein the external
2 source is a Global Positioning Satellite transmission.

1 73. The encoder of claim 47, wherein the digital data
2 is compressed using a compression standard resulting in a
3 compressed file, wherein the encoder further comprises:

4 means for creating a decompressed file prior to
5 signing the digital data;

6 means for signing the decompressed file resulting
7 in the digital signature; and

8 means for inserting the digital signature into a
9 header in the compressed file instead of inserting the same into
10 the digital data.

1 74. The encoder of claim 73, wherein the digital data
2 is an image and the compression standard is JPEG.

1 75. The encoder of claim 73, wherein the digital data
2 is video and the compression standard is MPEG.

1 76. The encoder of claim ⁴⁷ 50, wherein the digital data
2 is compressed using a compression standard resulting in a
3 compressed file, wherein the encoder further comprises:

4 means for creating a decompressed file prior to
5 signing the digital data;

6 means for inserting the associated data into the
7 decompressed file;

8 means for signing the decompressed file with the
9 associated data inserted therein resulting in the digital
10 signature; and

11 means for inserting the digital signature and
12 associated data into a header in the compressed file instead of
13 inserting the same into the digital data.

1 77. The encoder of claim 76, wherein the digital data
2 is an image and the compression standard is JPEG.

1 78. The encoder of claim 76, wherein the digital data
2 is video and the compression standard is MPEG.

1 79. The encoder of claim ⁴⁷ 50, wherein the digital data
2 comprises a plurality of samples, each of the samples being
3 defined by a plurality of bits, from a most significant bit
4 to a least significant bit, all of the least significant bits
5 defining the plurality of samples comprising a least significant
6 bit plane, wherein the encoder further comprises:

7 means for ignoring at least a portion of the least
8 significant bit plane in the digital data;

9 means for concatenating the associated data to the
10 digital data having the ignored least significant bit plane prior
11 to signing the digital data;

12 means for signing the digital data having the
13 concatenated associated data resulting in the digital signature;

14 wherein the predetermined bits comprise at least a
15 portion of the least significant bit plane and the associated
16 data is inserted into at least a portion of the remaining least
17 significant bits in the least significant bit plane.

1 80. The encoder of claim ⁴⁷ ~~50~~, further comprising:

2 means for providing time data identifying the time
3 the digital data was created;

4 means for concatenating the hash and the time
5 data;

6 means for applying a one-way hashing function to
7 the concatenated hash and time data resulting in a second hash;
8 and

9 means for encrypting the second hash instead of
10 the first hash to result in a time stamp containing the digital
11 signature, wherein both the digital data and the time data are
12 subsequently authenticated.

1 81. The encoder of claim 80, further comprising:

2 means for transmitting the hash to a third party
3 for providing the time stamp and concatenating the hash and time
4 stamp; and

5 means for receiving the second hash from the third
6 party prior to encryption.

1 82. The encoder of claim 81, wherein the trusted third
2 party resides at an internet address and the means for
3 transmitting and receiving is a computer capable of accessing the
4 internet and receiving the transmitted second hash.

1 83. The encoder of claim 80, further comprising a
2 semiconductor chip having a tamper resistant clock and a tamper
3 resistant time stamping circuit, wherein the clock outputs the
4 time data which together with the digital signature is signed by
5 the circuit to output the time stamp.

1 84. The encoder of claim ⁴⁷ 80, further comprising:

2 a memory for storing an identifier corresponding
3 to each of at least one user of a device which creates the
4 digital data;

5 recognition means for recognizing a user of the
6 device whose identifier is stored in the memory; and

7 output means for outputting the identifier
8 corresponding to the recognized user from the memory to be
9 inserted as the associated data.

1 85. The encoder of claim 84, wherein a private key for
2 signing the digital data is also stored in memory corresponding
3 to each user, wherein the identifier is inserted as associated
4 data and the private key is used to sign the digital data.

1 86. The encoder of claim 84, wherein the recognition
2 means is a fingerprint recognition system.

1 87. The encoder of claim 86, wherein the identifier is
2 a name of the recognized user.

1 88. A decoder for authenticating digital data having
2 an embedded digital signature in predetermined bits of the
3 digital data, the decoder comprising:

4 means for extracting the digital signature from
5 the predetermined bits;

6 means for decrypting the signature from the
7 digital data resulting in a first hash;

8 means for applying a one-way hashing function to
9 the digital data excluding the predetermined bits resulting in a
10 second hash; and

11 means for comparing the first hash to the second
12 hash wherein if the first hash matches the second hash the
13 digital data is authentic.

1 89. The decoder of claim 88, wherein the digital data
2 is selected from a group consisting of image data, video data,
3 and audio data.

1 90. The decoder of claim 88, wherein the digital data
2 further comprises associated data inserted into known bits of the
3 digital data wherein the decoder authenticates both the
4 associated data as well as the digital data.

1 91. The decoder of claim 90, wherein the associated
2 data is inserted into the bits of the digital data excluding the
3 predetermined bits.

1 92. The decoder of claim 90, wherein the digital data
2 is compressed using a compression standard resulting in a
3 compressed file and wherein the digital signature is contained in
4 a header in the compressed file, wherein the decoder further
5 comprises:

6 means for decompressing the compressed file; and

7 means for replacing the signature from the header
8 into the predetermined bits, prior to extracting the digital
9 signature from the predetermined bits.

1 93. The decoder of claim 90, wherein the digital data
2 is compressed using a compression standard resulting in a
3 compressed file and wherein the digital signature and associated
4 data are contained in a header in the compressed file, wherein
5 the decoder further comprises:

6 means for decompressing the compressed file; and

7 means for replacing the signature and associated
8 data from the header into the predetermined bits and the known
9 bits, respectively, prior to extracting the digital signature
10 from the predetermined bits.

1 94. A method for inserting data into digital data for
2 subsequent authentication of the digital data, the method
3 comprising the steps of:

4 receiving data from an external source;

5 inserting the data into the digital data; and

6 authenticating the digital data.

1 95. The method of claim 94, wherein the external
2 source is a radio frequency transmission.

1 96. The method of claim 94, wherein the external
2 source is an internet link.

1 97. The method of claim 94, wherein the inserted data
2 is used for authenticating information associated with the
3 digital data.

1 98. A device for inserting data into a digital data
2 for subsequent authentication of the digital data, the device
3 comprising:

4 means for receiving data from an external source;

5 means for inserting the data into the digital
6 image; and

7 means for authenticating the digital data.

1 99. The device of claim 98, wherein the external
2 source is a radio frequency transmission and the means for
3 receiving the data comprises an antenna.

1 100. The device of claim 98, wherein the external
2 source is an internet link and the means for receiving the data
3 comprises a computer capable of accessing the internet and
4 receiving the data.

1 101. The device of claim 98, wherein the inserted data
2 is used for authenticating information associated with the
3 digital data.

1 102. The device of claim 98, wherein the device is a
2 digital image generation device and the digital data represents
3 an image.

1 103. The device of claim 102, wherein the image
2 generation device is selected from a group consisting of a
3 digital camera, a digital video camera, and a digital scanner.

1 104. A method for inserting time data into digital data
2 for subsequent authentication of both the time data and the
3 digital data, the method comprising the steps of:

4 providing a semiconductor chip having a tamper
5 resistant clock and a time stamping circuit;

6 outputting the digital signature and time data
7 from the clock to the time stamping circuit;

8 signing the time data and the digital signature
9 resulting in a time stamp; and

10 authenticating the digital data and the time data.

1 105. A device for inserting time data into digital data
2 for subsequent authentication of both the time data and the
3 digital data, the device comprising:

4 a semiconductor chip having a tamper resistant
5 clock and a tamper resistant stamping circuit;

6 means for outputting the digital signature and
7 time data from the clock to the time stamping circuit; and

8 means for signing the time data and the digital
9 signature resulting in a time stamp.

1 106. The device of claim 105, wherein the device is a
2 digital image generation device and the digital data represents
3 an image.

1 107. The device of claim 106, wherein the image
2 generation device is selected from a group consisting of a
3 digital camera, a digital video camera, and a digital scanner.

1 108. A method for inserting data into digital data, the
2 device comprising:

3 storing an identifier corresponding to each of at
4 least one user of a device which creates the digital data;

5 recognizing a user of the device whose identifier
6 is stored in the memory;

7 outputting the identifier corresponding to the
8 recognized user from the memory; and

9 inserting data corresponding to the identifier
10 into the digital data.

1 109. The method of claim 108, wherein the inserted data
2 is used for authenticating the digital data.

1 110. The method of claim 108, wherein the inserted data
2 is used for authenticating information associated with the
3 digital data.

1 111. The method of claim 108, wherein the identifier is
2 a name of the recognized user.

1 112. A device for inserting data into digital data, the
2 device comprising:

3 a memory for storing an identifier corresponding
4 to each of at least one user of the device;

5 recognition means for recognizing a user of the
6 device whose identifier is stored in the memory;

7 means for outputting the identifier corresponding
8 to the recognized user from the memory; and

9 means for inserting data corresponding to the
10 identifier into the digital data.

1 113. The device of claim 112, wherein a private key for
2 signing the digital data is also stored in memory corresponding
3 to each user, wherein the identifier is inserted into the digital
4 data and the private key is used to subsequently sign the digital
5 data.

1 114. The device of claim 112, wherein the recognition
2 means is a fingerprint recognition means.

1 115. The device of claim 112, wherein the device is a
2 digital image generation device and the digital data represents
3 an image.

1 116. The device of claim 112, wherein the image
2 generation device is selected from a group consisting of a
3 digital camera, a digital video camera, and a digital scanner.

Add
DAJ